RE: Identity Theft

Dear Citizen:

I am writing in response to your inquiry regarding identity theft. Our best defense in helping Iowans with identity theft is to provide as much educational material as possible. In order to assist citizens who are concerned about identity theft, our office has prepared the enclosed brochures entitled, *A Guide for Victims of Identity Theft* and *Identity Theft... Don't Let It Happen To You.* The involvement of the Attorney General's Office in matters of identity theft is limited. We generally do not directly investigate identity theft.

The *Guide for Victims of Identity Theft* brochure outlines your rights, remedies and resources if someone is trying to collect a fraudulent debt. If you are still having problems after taking the steps outlined in the brochure, we suggest that you contact a private attorney for legal advice and/or assistance.

The *Identity Theft... Don't Let It Happen To You* brochure offers practical advice and precautionary steps you can take to reduce your risk of becoming a victim of identity theft. Please be aware that our office is continuing to explore the best ways to prevent identity theft and to help citizens who have been victims of identity theft. The information you provided will help us in that effort.

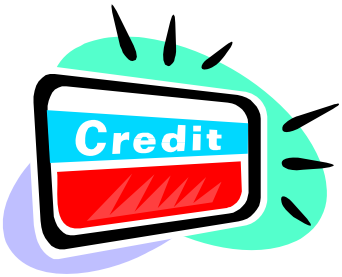
Thank you for contacting our office.

Sincerely,

Susan Kerr

Investigator

Enclosures



A GUIDE For Victims of Identity Theft

Iowa Attorney General
Consumer Protection Division
Hoover State Office Building
1305 East Walnut Street
Des Moines, Iowa 50319
www.IowaAttorneyGeneral.org
Consumer@AG.State.IA.US
515-281-5926
800-777-4590 Toll-free in Iowa

A Message from Attorney General Tom Miller

Dear fellow Iowans:

The goal of this brochure is to help you if you are a victim of "identity theft." Identity theft occurs when someone obtains important personal information, such as your Social Security number, birth date, banking or credit card account numbers, to commit fraud or theft.

"Identity thieves" commit a kind of financial sabotage. They use people's personal information to open fraudulent credit card accounts, rob retirement earnings, siphon money out of people's accounts, or commit other kinds of fraud.

The Consumer Protection Division of my office has developed this guide to provide you with information and steps to take if you are a victim; whom to contact, what to say, where to write or call, how to repair your credit record, and how to avoid future problems.

I am very sorry if you have been victimized by identity theft, and I sincerely hope the information in this guide will help you.

I encourage you to contact my office if we can provide any more information. Please log on to our website at www.IowaAttorneyGeneral.org for valuable information on identity theft as well as other consumer issues or write to the Consumer Protection Division, Hoover State Office Building, 1305 East Walnut Street, Des Moines, Iowa 50319, or call 515-281-5926.

With best wishes,

Tom Miller
Attorney General of Iowa

A GUIDE FOR VICTIMS OF IDENTITY THEFT

Identity theft crimes are on the rise, causing nationwide concern. Your personal identifying information can be accessed in an increasing variety of ways. An imposter can misuse your information to open fraudulent credit card accounts, secure deposits on cars and housing, obtain employment opportunities, create insurance benefits, and rob retirement earnings. This form of financial sabotage can devastate your credit and require endless hours of telephone and written communication to resolve. In the meantime, you may experience difficulty writing checks, obtaining loans, renting apartments, and even getting hired.

This guide provides victims of identity theft with clear and concise information, and the major resources to contact to resolve the conflicts which remain long after the thief disappears. Unfortunately, the responsibility of identifying and resolving the consequences of identity theft is left largely to the victims themselves. It is important to act quickly and assertively to minimize the damage to your credit reputation. While identity theft is a "crime" which law enforcement officials can prosecute, the perpetrator is often difficult to track. In addition, law enforcement officials cannot clean up the havoc created for you.

In dealing with the authorities and financial institutions, ***keep a log*** *of all conversations, including dates, names, and telephone numbers. Keep notes on the time spent and any expenses incurred. Confirm all conversations in writing. Send correspondence by certified mail (return receipt requested). Keep copies of all letters and documents.*

---

1. Credit bureaus. Immediately call the fraud units of the three credit reporting bureaus -- Equifax, Experian, and Trans Union. Report the theft of your credit cards or misuse of your account numbers. Ask each agency to place a "FRAUD ALERT" on your credit report and send you a copy of your credit file. Your telephone call will place a temporary (90-day) fraud alert on your credit file. You MUST follow the telephone call up with a completed ID Theft Affidavit (which is enclosed) and request a permanent fraud alert (7 year) and add a FRAUD VICTIM STATEMENT which can only be done in writing. The victim statement can contain up to 100 words and should give a brief summary of your circumstances such as: "My identification has been used to apply for fraudulent credit. Be sure to add: "Do NOT extend any existing lines of credit or open any new lines of credit without contacting me personally at [your mailing address and a couple of telephone numbers where you can be reached most of the time]. to verify ALL applications and/or actions taken!" Be sure to ask for a permanent (7 year) fraud alert on your credit file, and how you can extend it if necessary.

Be aware that these measures may not entirely stop fraudulent new accounts from being opened by the identity thief. Ask the credit reporting bureaus, in writing, to provide you with copies every few months so you can monitor your credit filet. Upon your request, a credit bureau is required to provide you with one *free* credit report during any 12-month period if you have reason to believe the report contains inaccurate information due to fraud. Additional credit reports shall not exceed an $9.00 charge and this fee is often waived. (15 United States Code section 1682j(c)(3))

Request the credit bureaus, in writing, to provide you the names and phone numbers of credit grantors with whom fraudulent accounts have been opened. Request the credit bureaus, in writing, to remove inquiries that have been generated due to the fraudulent access. Request that all fraudulent information and inquiries be permanently removed from your credit report. You may also request the credit bureaus to notify those who have received your credit report in the last six months in order to alert them to the disputed and erroneous information (two years for employers).

Credit Bureau	Report Consumer Fraud	Request Credit Report	Get Off Mailing Lists
Equifax P.O. Box 740256 Atlanta, GA 30374 www.equifax.com	888-766–0008 and write to address at left.	800-685-1111	888-567-8688 -or- log on to: www.optoutprescreen.com -or- write to: Equifax, Inc. Options P.O. Box 740123 Atlanta, GA 30374
Experian P.O. Box 9530 Allen, TX 75013 www.experian.com	888-397-3742 and write to address at left.	888-397-3742	888-567-8688 -or- log on to: www.optoutprescreen.com -or- write to: Experian Consumer Opt-Out 701 Experian Parkway Allen, TX 75013
Trans Union P.O. Box 6790 Fullerton, CA 92834 www.transunion.com	800-680-7289	800-916-8800	888-567-8688 -or- log on to: www.optoutprescreen.com -or- write to: TransUnion Corporation Name Removal Option P.O. Box 505 Woodlyn, PA 19094

2. Creditors. Contact all creditors *immediately* with whom your name has been used fraudulently -- by telephone AND in writing. Get replacement cards with new account numbers for your own accounts that have been used fraudulently. Ask that old accounts be processed as "account closed at consumer's request." This is better than "card lost or stolen," because when this statement is reported to credit bureaus, it can be interpreted as blaming you for the loss. Carefully monitor your mail and credit card statements for evidence of new fraudulent activity. Report it immediately to credit grantors.

Victims of unauthorized use of a credit card will be liable for no more than the first $50 of the loss, although this is often waived and victim will not be required to pay any part of the loss. (15 United States Code section 1643)

Request the credit grantor to provide you with a copy of the fraudulent credit application and a statement of the incurred charges. Such information may be helpful in disputing the application and/or charges as fraudulent. If the credit grantor resists providing you this information, contact your local police or sheriff's department for assistance. The credit grantor should readily provide such information when requested to do so by local law enforcement authorities.

Pay particular attention to what personal identifying information the identity thief has provided on the application and note any discrepancies that may exist. When reviewing the charges, note the date of the purchases, where the purchases were made and what type of products or services were purchased. Look for dates, places or items which contradict your own schedule, whereabouts, and even tastes.

Credit requirements to verify fraud: You may be asked by banks or credit grantors to fill out and notarize fraud affidavits, such as the one that enclosed. Find out if the creditor accepts this affidavit and whether they require notarization or a police report. An affidavit with supporting documentation and a police report should be enough. Overly burdensome requirements by banks or creditors should be reported to the government authority which regulates the credit card issuer. To determine which authority regulates the particular credit card issuer in question, contact:

Iowa Department of Commerce
Banking Division
200 E. Grand, Suite 300
Des Moines, IA 50309-1827
Phone: 515-281-4014
www.idob.state.ia.us

3. Law enforcement: Report the crime to all police and sheriff's departments with jurisdiction in your case. Give them as much documented evidence as possible. Get a copy of your police report. Keep the telephone number of your fraud investigator handy and give it to creditors and others who require certification of your case. Banks and credit card companies may require you to produce the police report in order to verify the crime.

4. Stolen checks: If you have had checks stolen or bank accounts set up fraudulently, report it to the check verification companies listed below. Put stop payments on any outstanding checks that you are unsure of. Cancel your checking and savings accounts and obtain new account numbers. Give the bank a secret password for your account. When creating a password, don't use common numbers like the last four digits of your Social Security number, your birth date, middle name, mother's maiden name, pet's name, address, consecutive numbers, or anything else that could easily be discovered by thieves.

Check Verification Company	Telephone Number	Mailing Address
CheckRite/Global Payments www.globalpaymentsinc.com	800-638-4600 800-766-2748	6515 West Howard Street Niles, IL 60714
ChexSystems www.chexhelp.com	800-428-9623	7805 Hudson Road, Suite 100 Woodbury, MN 55125
Certegy (formerly Equifax) www.certegy.com	800-437-5120	P.O. Box 30272 Tampa, FL 33630
SCAN www.scanassist.com	877-382-7226 800-262-7771	7805 Hudson Road, Suite 100 Woodbury, MN 55125
TeleCheck (formerly NPC/ICS) www.telecheck.com	800-366-2425 800-710-9898	5251 Westheimer Houston, TX 77056

5. Automatic Teller Machine (ATM) cards: If your ATM card has been stolen or compromised, get a new card, account number and password. Do not use your old password or the common passwords and personal identification numbers listed above.

6. Fraudulent change of address, mail theft, or other mail involvement: Notify the U.S. Postal Inspector's Office for Iowa if you suspect an identity thief has filed a change of address with the post office or has used the mail to commit bank or credit fraud. Theft of mail is a felony. Find out where the fraudulent credit cards were sent. Notify the local Postmaster for that address to forward all mail in your name to your *own* address. You may also need to talk with the local mail carrier for that address as well.

U.S. Postal Inspectors
P.O. Box 566
Des Moines, IA 50302-0566
Phone: 515-253-9060
www.usps.com/postalinspectors

7. Secret Service jurisdiction: The Secret Service investigates crimes dealing with credit card fraud, financial institution fraud, and crimes dealing with the false use of personal identifiers (such as name, date of birth, or Social Security number) relating to financial crimes. However, the Secret Service usually does not investigate individual cases unless the dollar amount is high or you are one of many victims of a fraud ring. If the actual crime (fraudulent application or charges) occurred outside of Iowa, the Secret Service may forward your case to the appropriate office.

U.S. Secret Service
210 Walnut Street, Room 637
Des Moines, IA 50309
Phone: 515-284-4565
www.secretservice.gov

8. Social Security Number misuse: To determine is someone is misusing your Social Security number for employment purposes, order a copy of your *Social Security Statement* from Social Security Administration to check for inaccuracies or fraud. To request a *Statement* call or write to the office listed below. Once you have determined that there are too many or too few earnings are recorded on your *Statement*, or if your name is recorded incorrectly, call or write to:

Social Security Administration
Office of the Inspector General (OIG)
210 Walnut Street, Room 293
Des Moines, IA 50309
Phone: 800-772-1213
515-283-0212
website to download a *Statement* application:
http://www.socialsecurity.gov

If some is misusing your Social Security number, as a last resort, you may consider changing your number. The Social Security Administration will change your number only if you fit specific fraud victim criteria. For more information, call or write the office listed below and request the fact sheet, Social Security: When Someone Misuses Your Social Security Number, SSA Pub. No. 05-10064. Report the fraudulent use of your Social Security number to:

Social Security Administration
Office of the Inspector General (OIG)

P.O. Box 17768
Baltimore, MD 21235
Phone: 800-269-0271 (OIG Fraud Hotline)
e-mail: oig.hotline@ssa.gov

9. Income tax fraud: Any fraudulent use of another person's Social Security number, including dependents' Social Security numbers, to obtain an income tax refund should be reported to:

Internal Revenue Service
210 Walnut Street, Room 147
Des Moines, IA 50309
Phone: 515-284-4240

Internal Revenue Service
Criminal Investigation Division
P.O. Box 7908, Stop 9000
Shawnee Mission, KS 66207-7909
Phone: 800-829-0433
www.irs.gov

10. Passports: If you are the victim of identity theft and have a passport, notify the passport office, in writing, to be on the lookout for anyone ordering a new passport fraudulently.

U.S. Postal Service
Passport Acceptance Unit
1165 - 2nd Avenue, Room 228
Des Moines, IA 50318-9802
Phone: 515-283-7742

U.S. Department of State Passport Services
Consular Lost/Stolen Passport Section
1111 - 19th Street N.W., Suite 500
Washington, DC 20036
Phone: 202-955-0487
www.state.gov/travel

11. Utilities: If your cellular phone or long distance calling card has been stolen or if you discover fraudulent charges on your bills, cancel the accounts and open new ones. To avoid being "slammed," request that your local telephone service "freeze" your long distance carrier so it cannot be changed without specific authorization using a password. To avoid being "crammed," scrutinize every charge on your billing statements for fraudulent or unauthorized charges. Notify your gas, electric, water, and trash utilities that you are a victim of identity theft and alert them to the possibility that the thief may try to establish accounts using your personal information.

12. Driver's license number misuse: You may need to change your driver's license number if someone is using yours fraudulently. Call the Iowa Department of Transportation's Motor Vehicle Information Center and verify the last issuance date of your license. If there is a discrepancy and you have a non-commercial driver's license, go to your local driver's license station and apply for a

duplicate license with an "assigned" number. Commercial drivers will be unable to use an "assigned" number, but should contact the Motor Vehicle Enforcement Office to file a fraud report. Send a letter, complete with supporting documents, requesting a fraud investigation to:

Iowa Motor Vehicle Enforcement
P.O. Box 10473
Des Moines, IA 50306-0473
Phone: 515-237-3247
Phone: 800-925-6469 (toll-free within Iowa)
www.dot.state.ia.us/mvd/omve

13. False civil and criminal judgments: Sometimes victims of identify theft are wrongfully accused of crimes committed by the imposter. If a civil judgment has been entered against you for actions taken by your imposter, contact the court where the judgment was entered and report that you are a victim of identify theft. If you are wrongfully prosecuted for criminal charges, contact the Federal Bureau of Investigation (FBI). Ask how to clear your name.

U.S. Federal Bureau of Investigation
3737 Woodland Avenue
West Des Moines, IA 50266
Phone: 515-223-4278
If no answer call Omaha, NE
Phone: 402-493-8688
www.fbi.gov

14. Credit report fraud: The Federal Trade Commission (FTC) maintains the Identity Theft Data Clearinghouse, the federal government's centralized identity theft complaint database, and provides information to identity theft victims. The FTC collects complaints from identity theft victims and shares their information with law enforcement nationwide. This information also may be shared with other government agencies, consumer reporting agencies, and companies where fraud was perpetrated to help resolve identity theft related problems. If you find that there has been unauthorized access or use of your *credit report*, the Federal Trade Commission will be able to advise you of your rights under the Fair Credit Reporting Act. Call or write to:

Federal Trade Commission
Identity Theft Clearinghouse
600 Pennsylvania Avenue N.W.
Washington, DC 20580
Phone: 877-438-4338 (toll-free)
www.consumer.gov/idtheft

15. Insurance coverage: You may want to consult with your insurance agent to determine whether your losses may be covered by household or other insurance policies.

16. Legal help: You may want to consult with a private attorney to determine legal action to take against creditor grantors and/or credit bureaus if they are not cooperative in removing fraudulent entries from your credit report or if negligence is a factor. An attorney can help you recover from the fraud and determine whether your rights under various credit, banking, Social Security, and other laws have been violated. The Iowa State Bar Association will provide you with the name of one

attorney in your area that handles consumer protection issues. If you should decide to consult with the attorney to whom you were referred, this service ensures that you will not be charged more than $25.00 for the first half hour consultation. Call or write to:

Iowa State Bar Association
Lawyer Referral Service
521 E. Locust Street, 3rd Floor
Des Moines, IA 50309
Phone: 800-532-1108 or www.iowabar.org

17. Legal remedies: Identity theft is a crime in Iowa with both civil and criminal penalties.

If you wish to pursue a civil remedy, you may consider filing your case through Small Claims Court. The maximum allowable claim is $5,000 in Iowa. This private action would permit you to recover $1,000 or three times the actual damages, whichever is greater along with reasonable attorney fees and court costs. Small claims court procedures are designed for people to pursue their claims without an attorney's help, although representation by an attorney in small claims court is also allowed. Your claim can be filed through the Clerk of Court in the county where the theft took place. The Clerk's Office will provide you with the necessary forms and information throughout the process. You may also consider contacting a private attorney for advice and assistance in determining your rights and remedies. If your claim is for more than $5,000, you will need to contact a private attorney to file a claim in District Court. Refer to section sixteen (16) for the Iowa State Bar Association's Lawyer Referral Service or another option would be to check the yellow page listings under attorneys or lawyers in your local telephone directory.

If you wish to pursue a criminal remedy, you may consider filing a report with the law enforcement agency where the identity thief resides for possible prosecution under that state's laws. The law enforcement agency will review your case with the county or district attorney who has primary jurisdiction in filing criminal charges in that locale.

IOWA'S IDENTITY THEFT LAW

714.16B IDENTITY THEFT -- CIVIL CAUSE OF ACTION.

In addition to any other remedies provided by law, a person as defined under section 714.16, subsection 1, suffering a pecuniary loss as a result of an identity theft by another person under section 715A.8, or a financial institution on behalf of an account holder suffering a pecuniary loss as a result of an identity theft by another person under section 715A.8, may bring an action against such other person to recover all of the following:

1. Five thousand dollars or three times the actual damages, whichever is greater.
2. Reasonable costs incurred due to the violation of section 715A.8, including all of the following:
    a. Costs for repairing the victim's credit history or credit rating.
    b. Costs incurred for bringing a civil or administrative proceeding to satisfy a debt, lien, judgment, or other obligation of the victim.
    c. Punitive damages, attorney fees, and court costs.

For purposes of this section, "financial institution" means the same as defined in section 527.2, and includes an insurer organized under Title XIII, subtitle 1, of this Code, or under the laws of any other state or the United States.

99 Acts, ch 47, §1; 2005 Acts, ch 18, §2

Referred to in § 614.4A

715A.8 IDENTITY THEFT.

1. a. For purposes of this section, "identification information" includes, but is not limited to, the name, address, date of birth, telephone number, driver's license number, nonoperator's identification card number, social security number, student identification number, military identification number, alien identification or citizenship status number, employer identification number, signature, electronic mail signature, electronic identifier or screen name, biometric identifier, genetic identification information, access device, logo, symbol, trademark, place of employment, employee identification number, parent's legal surname prior to marriage, demand deposit account number, savings or checking account number, or credit card number of a person.

b. For purposes of this section, "financial institution" means the same as defined in section 527.2, and includes an insurer organized under Title XIII, subtitle 1, of this Code, or under the laws of any other state or the United States.

2. A person commits the offense of identity theft if the person fraudulently uses or attempts to fraudulently use identification information of another person, with the intent to obtain credit, property, services, or other benefit.

3. If the value of the credit, property, or services exceeds one thousand dollars, the person commits a class "D" felony. If the value of the credit, property, or services does not exceed one thousand dollars, the person commits an aggravated misdemeanor.

4. A violation of this section is an unlawful practice under section 714.16.

5. Violations of this section shall be prosecuted in any of the following venues:

a. In the county in which the violation occurred.

b. If the violation was committed in more than one county, or if the elements of the offense were committed in more than one county, then in any county where any violation occurred or where an element of the offense occurred.

c. In the county where the victim resides.

d. In the county where the property that was fraudulently used or attempted to be used was located at the time of the violation.

6. Any real or personal property obtained by a person as a result of a violation of this section, including but not limited to any money, interest, security, claim, contractual right, or financial instrument that is in the possession of the person, shall be subject to seizure and forfeiture pursuant to chapter 809A. A victim injured by a violation of this section, or a financial institution that has indemnified a victim injured by a violation of this section, may file a claim as an interest holder pursuant to section 809A.11 for payment of damages suffered by the victim including costs of recovery and reasonable attorney fees.

7. A financial institution may file a complaint regarding a violation of this section on behalf of a victim and shall have the same rights and privileges as the victim if the financial institution has indemnified the victim for such violations.

8. Upon the request of a victim, a peace officer in any jurisdiction described in subsection 5 shall take a report regarding an alleged violation of this section and shall provide a copy of the report to the victim. The report may also be provided to any other law enforcement agency in any of the jurisdictions described in subsection 5.

99 Acts, ch 47, §2; 2003 Acts, ch 49, §1; 2005 Acts, ch 18, §3, 4
Referred to in § 714.16B, 715A.9A

715A.9 VALUE FOR PURPOSES OF IDENTITY THEFT.
The value of property or services is its highest value by any reasonable standard at the time the identity theft is committed. Any reasonable standard includes but is not limited to market value within the community, actual value, or replacement value. If credit, property, or services are obtained by two or more acts from the same person or location, or from different persons by two or more acts which occur in approximately the same location or time period so that the identity thefts are attributable to a single scheme, plan, or conspiracy, the acts may be considered as a single identity theft and the value may be the total value of all credit, property, and services involved.

99 Acts, ch 47, §3

18. Making changes: New laws regarding right to privacy issues and fraud victim assistance programs are currently being drafted and proposed at the federal and state levels of government. If you are disappointed with the privacy protection and fraud assistance available under current laws, consider writing your federal and state legislators concerning your experience. To obtain a list of **Iowa** Senators and Representatives, log on to www.legis.state.ia.us. To obtain a list of **U.S.** Senators and Representatives, log on to www.firstgov.gov.

19. Don't give in: Remember, you are not responsible for any bill, portion of a bill, or checks written or cashed which result from identity theft. Your credit rating should not be permanently affected, and no legal action should be taken against you. If any merchant, financial institution or collection agency suggests otherwise, simply restate your willingness to cooperate, but don't allow yourself to be coerced into paying a fraudulent debt. Many victims of identity theft report feeling angry, frustrated, powerless, and even violated. If these feelings persist or become overwhelming, talk to your friends, family members, or a counselor.

If you have any further questions or concerns,
or if you would like additional information, please contact:

Iowa Attorney General Tom Miller
Consumer Protection Division
1300 East Walnut
Hoover State Office Building
Des Moines, IA 50319
www.IowaAttorneyGeneral.org
Consumer@AG.State.IA.US
515-281-5926

This publication originates from the California Public Interest Research Group (CALPIRG), 11965 Venice Blvd., Ste. 408, Los Angeles, CA 90066, Phone: 310-397-3404; web site: www.pirg.org/calpirg, and Privacy Rights Clearinghouse, 5384 Linda Vista Rd., Ste. 306, San Diego, CA 92110, Phone: 619-298-3396, e-mail: www.privacyrights.org. With their consent, it has been adapted for Iowa consumers, edited and distributed by the Consumer Protection Division of the Office of Attorney General Tom Miller, Iowa Department of Justice.
August 2007

IDENTITY THEFT...
Don’t let it happen to YOU!

Iowa Attorney General
Consumer Protection Division
Hoover State Office Building
1305 East Walnut Street
Des Moines, Iowa 50319
www.IowaAttorneyGeneral.org
Consumer@AG.State.IA.US
515-281-5926
800-777-4590 Toll-free in Iowa

A Message from Attorney General Tom Miller

Dear fellow Iowans:

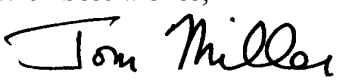
The goal of this brochure is to help you avoid becoming a victim of "identity theft." Identity theft occurs when someone obtains important personal information, such as your Social Security number, banking or credit card account numbers, to commit fraud or theft.

Today's credit identity thieves are information seekers and they don't need to steal your wallet. They obtain bits of information by sorting through trash for discarded receipts and statements, spying for your PIN number at ATM machines or telephone booths, accessing public records, and even stealing from your mailbox.

The Consumer Protection Division of my office developed this brochure to suggest steps you can take to reduce your risk of disclosing important personal information and of becoming a victim of identity theft.

I encourage you to contact my office if we can provide any more information. Please log on to our website at www.IowaAttorneyGeneral.org for valuable information on identity theft as well as other consumer issues or write to the Consumer Protection Division, Hoover State Office Building, 1305 East Walnut Street, Des Moines, Iowa 50319, or call 515-281-5926.

With best wishes,



Tom Miller
Attorney General of Iowa

IDENTITY THEFT... DON'T LET IT HAPPEN TO YOU!

Identity theft crimes are on the rise causing nationwide concern. Your personal identifying information can be accessed in a variety of ways. An imposter can misuse your information to open fraudulent credit card accounts, secure deposits on cars and housing, obtain employment opportunities, create insurance benefits, and rob retirement earnings. This form of financial sabotage can devastate your credit and require endless hours of telephone and written communication to resolve. In the meantime, you may experience difficulty writing checks, obtaining loans, renting apartments, and even getting hired. While following these precautionary steps is not a guarantee, it will greatly reduce your chances of becoming the next identity theft victim.

Reducing access to your personal identifying information:

1. To minimize the amount of information a thief can steal, do not carry extra credit cards, your Social Security card, birth certificate, or passport in your wallet or purse, except when needed.

2. To reduce the amount of personal information that is "out there," consider the following:

- Remove your name from the marketing lists of the three credit reporting bureaus -- Equifax, Experian, and Trans Union. This will limit the number of pre-approved credit offers that you receive in the mail. Financial institutions mail over 3 billion pre-approved credit offer a year! When in transit or tossed into the garbage, such solicitations are a likely target of identity thieves who use them to order credit cards in your name. To remove your name:

  Call toll-free 888-567-8688 -or-

  Log on to website www.optoutprescreen.com -or-

  Write to:

Equifax, Inc.	Experian	TransUnion Corporation
Options	Consumer Opt Out	Name Removal Option
P.O. Box 740123	701 Experian Parkway	P.O. Box 505
Atlanta, GA 30374	Allen, TX 75013	Woodlyn, PA 19094

- Order your credit report once a year from each of the three credit bureaus to check for inaccuracies and fraudulent use of your accounts. Monitoring your credit card statements and your credit report are the most important steps you can take to safeguard your credit identity. The three credit bureaus are competitors who collect data independently. Thus, all three credit reports must be reviewed to ensure the accuracy and safety of your profile.

Credit Bureau	Report Consumer Fraud	Request Credit Report	Website Access
CSC Credit Services (Equifax Regional Office) P.O. Box 619054 Dallas, TX 75261	800-272-9281	800-759-5979	www.csccredit.com
Equifax P.O. Box 740256 Atlanta, GA 30374	888-766-0008	800-685-1111	www.equifax.com
Experian P.O. Box 9530 Allen, TX 75013	888-397-3742	888-397-3742	www.experian.com
Fair Isaac Credit Score 901 Marquette Ave, Ste3200 Minneapolis, MN 55402	----------	800-777-2066	www.fairisaac.com
Trans Union P.O. Box 6790 Fullerton, CA 92834	800-680-7289	800-916-8800	www.transunion.com

- Put your telephone number on the **National Do Not Call Registry**. The Federal Trade Commission (FTC), the Federal Communications Commission (FTC), and the states Attorney Generals are enforcing the National Do Not Call Registry to make it easier and more efficient for you to stop getting telemarketing calls you don't want. Placing your number on the registry will stop most, but not all, telemarketing calls. Registration is free and you can

Register online at www.DoNotCall.gov	Register up to 3 telephone numbers and you will receive a confirmation by e-mail.
Call toll-free 888-382-1222	You must call from the telephone number that you wish to register.

- Remove your name, home mailing address, home telephone number, and home e-mail address from many national lists by opting out of the Direct Marketing Association's marketing lists. The Direct Marketing Association is the largest national trade association serving the direct and interactive marketing field. This service is only available for individuals and "home" addresses (not businesses). You will be removed from the Direct Marketing Association member lists for five (5) years.

To remove your name from national mailing lists for a $1 fee by mail, write:	Mail Preference Service Direct Marketing Association P.O. Box 282 Carmel, NY 10512-0643

Or remove your name from national mailing and e-mail lists for a $1 fee, on-line:	www.the-dma.org

- Consider removing your name and address from the telephone book, reverse directories, and city directories. By eliminating your name from these sources, you can reduce access to your personal information from places like the Internet (which mainly use public information resources as a database), telemarketers, and identity thieves.

To block your address, call or write:	Qwest/Dex 1-800-244-1111 McLeod Yellow Book USA 800-373-2324	No fee
To remove your information from the phone book ("non-listed"), call or write:	Qwest/Dex 1-800-244-1111 McLeod Yellow Book USA 800-373-2324	$2.50 monthly
To remove your information from the phone book and directory assistance ("non-published"), call or write:	Qwest/Dex 1-800-244-1111 McLeod Yellow Book USA 800-373-2324	$4.00 monthly
To remove your information from the city directory, call or write:	R. L. Polk Company 37001 Industrial Road Livonia, MI 48150 1-800-275-7655	Free

- Iowa law allows individuals to utilize an "assigned" driver's license number rather than using their Social Security number. The Social Security number is the most frequently used record keeping number in the United States. The widespread use of Social Security numbers makes invasion of privacy and fraud easier to commit. Even though you are given an assigned number, Iowa law requires you to *disclose* your Social Security number to the Department of Transportation when applying for an Iowa driver's license. In addition to being your driver's license number, an assigned number can be utilized in a variety of ways, thus protecting your Social Security number from unnecessary public disclosure. Iowa law protects your personal identifying information on your driver's license from public disclosure. (Iowa Code section 321.11) However, personal information does not include your factual driving record (such as records of conviction or occurrences of accidents). To report driver's license fraud, contact:

Iowa Department of Transportation

Office of Driver Services

6310 S.E. Convenience Blvd.

Ankeny, IA 50021

Phone: 515-244-8725

Phone: 800-532-1121 (toll-free within Iowa)

www.dot.state.ia.us

- Iowa law allows individuals to delete their Social Security number, middle name (you may consider using a middle initial if you have a common name) and telephone number from voter registration records. (Iowa Code section 48A.11) Your local County Auditor's Office can give you or mail you a Voter Registration Application to change the information contained within your voter registration file. Fill out the entire form and simply write "delete" in the areas you want to protect from public disclosure. This form is also available in most Qwest Dex and Telecom telephone books in the government listings.

3. Install a locked mailbox, a front door slot at your residence to reduce mail theft, or use a post office box. When you pay bills, do not leave the envelopes containing your checks at your homes mailbox for the postal carrier to pick up. If stolen, your checks can be altered and then cashed. If stolen, credit card payments contain all the necessary information an identity thief needs. Never write your credit card account number or Social Security number on your checks when making a payment. Due to an increased risk of theft and vandalism, it is best to mail bills and other sensitive items at the post office, rather than from your residence or neighborhood drop boxes.

4. When you order new checks, consider removing "extra" information such as your Social Security number, assigned driver's license number, middle name, and telephone number. The less personal identifying information you make available, the more likely an identity thief will choose an easier target. Do not have new checks sent to your homes mailbox. Pick them up at the bank instead.

Credit cards:

5. Reduce the number of credit cards you actively use to a bare minimum. Carry only one or two of them in your wallet. Cancel all unused accounts. Even though you do not use them, their account numbers are recorded in your credit report, which is full of data that can be used by identity thieves. Cut up the unused card, return it to the credit card issuer and request that the account by “closed at customer’s request”.

6. Keep a list or photocopy of all your credit cards, account numbers, expiration dates, and telephone numbers of the customer service and fraud departments in a secure place (not your wallet or purse) so you can quickly contact your creditors in case your cards have been lost or stolen. Do the same with your bank accounts.

7. Never give out your credit card number or other personal information over the telephone unless you have a trusted business relationship with the company and **YOU HAVE INITIATED THE CALL**. Identity thieves have been known to call their victims with a fake story that goes something like this: "Today is your lucky day! You have been chosen by the Publishers Consolidated Sweepstakes to receive a free trip to the Bahamas. All we need is your credit card number and expiration date to verify you as the lucky winner." Identity thieves tell you they are the IRS, your credit card fraud department, the hospital emergency room, or anyone else they can pretend to be to "panic" you in to giving up your personal information.

8. Always take credit card and ATM receipts with you. Never toss them in a public trash container.

9. You will receive "Privacy Notices" once a year from businesses that you have a financial relationship with. The Privacy Notice tells you whether the business shares information that it knows about you with other businesses. In many cases, if you fail to respond to the Privacy Notice you are allowing that business to share, sell, or trade YOUR personal information to ANYONE! So the next time you receive a Privacy Notice, read the back page and make an affirmative decision on whether you want that business to share your personal information.

10. If your credit card issuer sends random issue convenience checks, request (in writing) to be removed from the mailing list. Credit card convenience checks are easy prey for identity thieves to steal and use while often times, the consumer is unaware that the random checks were even issued. Your credit card billing statement should contain a different address for "correspondence" to the issuer. Do not send your requests to the same address where you send your credit card payments.

11. Watch the mail when you are expecting a new credit card that you have applied for or a reissued credit card that has expired. Immediately contact the issuer if the credit card does not arrive.

12. One of the benefits for consumers using the Internet, a global network of interlinked computer networks, is the ability to purchase products and services around the clock electronically from the convenience of their home or office. One of the drawbacks is the potential for fraud and deception. Be careful when using a credit card or before providing personal information (such as your Social Security number or date of birth) on the Internet. Read the browser's and the merchant's security and/or privacy statement. Look for the words Secure Sockets Layer (SSL) or Secure Electronic Transaction (SET) to establish if the website is encrypted

which means that is secure from unauthorized parties. Look for the symbols of a padlock or key in the lower right hand corner of your browser window (whether you see a padlock or a key depends on which browser you are using). If the padlock or the key are unbroken, the website is secure. Check to see if the web address includes an "s" for example https://. The "s" indicates that the website contains SSL or SET and is secure.

Passwords and Personal Identification Numbers (PINs):

13. Avoid using common, easy to guess passwords and PINs such as the last four digits of your Social Security number, your birth date, middle name, mother's maiden name, pet's name, address, consecutive numbers, or anything else that could be discovered easily by thieves.

14. Ask your financial institution to add extra security protection to your account. Most will allow you to use an additional code (a number or word) when accessing your account. Do not use the common passwords and PINs listed above.

15. Memorize all of your passwords. Don't record them on anything in your wallet or purse.

16. Shield your hand when using your PIN at an ATM, a point of sale terminal at the store, or when making long distance phone calls with your phone card. "Shoulder surfers" may be spying nearby with binoculars or a video camera.

Social Security numbers:

17. Protect your Social Security number. Release it only when when required by law (such as tax forms, employment records, banking/stock/property transactions, driver's/marriage/professional license applications, etc.) or when in your best interest. If a government agency requests important personal information, including your Social Security number, a Privacy Act notice should accompany the request. (5 United States Code section 552a(e)(3)) This notice will explain whether disclosure of such information is required or requested, the use that will be made of the information, and what will happen if you refuse to provide all or any part of the information. Your Social Security number is the key to most of your personal records such as your financial accounts, medical and insurance records, and government files making it a prime target of identity thieves. You may wish to utilize an "assigned" driver's license number rather than your Social Security number whenever possible.

18. Do not have your Social Security number pre-printed on your checks. Ask that merchants not hand-write your Social Security number on your checks because of the risk of fraud. Currently, there is no law against a merchant requiring you to divulge your Social Security number before accepting a check, so you may need to be assertive. Offering an assigned driver's license number is usually an adequate substitute.

19. Review your annual *Social Security Statement* for inaccuracies or fraud. You will receive your *Statement* from the Social Security Administration automatically each year about three months before your birthday if you:

- are age 25 or older
- have worked in Social Security-covered employment or self-employment,
- are not yet receiving benefits

- have a current mailing address on file

If you have not received your ***Statement*** or have questions, check the website, write, or call:

Social Security Administration
Office of the Inspector General
210 Walnut Street, Room 293
Des Moines, IA 50309
Phone: 800-772-1213
515-283-0212
www.SocialSecurity.org

Responsible information handling:

20. Carefully review your credit card statements and phone bills, including cellular phone bills, for unauthorized charges or fraudulent use. Be aware that under current laws, your local telephone company is obliged to let other carriers use their billing systems for a fee. More and more unscrupulous third parties are billing consumers for goods such as; special services, calling plans, or memberships that they did not order and do not want (commonly called "cramming"). Many unauthorized charges result from "free" trial offers which are always followed by some type of charge following the brief trial period... because the goods or services are never really "free". Scrutinize your local, long distance and cellular telephone bills each month for fraudulent or unauthorized charges. Be aware that some long distance telephone companies resort to deceptive tactics to switch your service without authorization (commonly called "slamming"). You may contact your local telephone company to verify your long distance carrier and request a "freeze" on your account so it cannot be changed without your specific authorization using a password.

21. Do not toss credit card convenience checks or pre-approved credit offers in your trash or recycling bin without first tearing them into small pieces or shredding them. They can be used by "dumpster divers" to cash the checks or order credit cards in *your* name and mail them to *their* address. Do the same with other sensitive information like credit card receipts, banking statements, utility bills, and so on. Home shredders can be purchased in most office supply and discount stores for a minimum cost. By adopting responsible information handling practices, you can reduce the risk of fraud.

22. When you fill out credit or loan applications, find out how the company disposes of them. If you are not convinced that they store them in locked files and/or shred all paper records before discarding them, take your business elsewhere. Some auto dealerships, department stores, car rental agencies, and video stores have been known to be careless with customer applications or an employee at the business with "insider access" may retrieve your personal information to sell or use fraudulently. When you pay by credit card, ask the business how it stores and disposes of the transaction slip. Avoid paying by a check or debit card if you think the business does not use adequate safeguards.

23. Store your canceled checks in a safe place. In the wrong hands, they could reveal a lot of about you, including information about your other accounts by looking through the payments you have made, so avoid writing individual account numbers on the "memo" portion of each check. Never permit your credit card number to be written onto your checks. Iowa law prohibits a merchant from recording your credit card number or expiration date as a condition of acceptance of a check for the sale of goods or services. Iowa law does NOT prohibit a merchant from requesting that you display a credit card, and it allows the merchant to record only the name and issuer (bank name) of the credit card. However, a credit card number may be requested and recorded in lieu of a deposit to secure payment in the event of loss, damage, or default. (Iowa Code section 537.8101)

24. "Privacy notices" are being mailed to consumers annually in their bank statements, credit card statements, investment reports, mortgage statements, insurance mailings and so on. The Financial Services Modernization Act (also known as Gramm-Leach-Bliley or GLB)(15 U.S.C. sections 6801-6810) requires banks and other companies that provide financial services and products to tell their customers three things:

> **1. Privacy Policy:** Your financial institution must tell you the kinds of information it collects about you and how it uses that information.
>
> **2. Right to Opt-Out:** Your financial institution must explain your ability to prevent the sale of your personal information to third parties.
>
> **3. Safeguards**: Financial institutions are required to develop policies to prevent fraudulent access to confidential financial information. These policies must be disclosed to you

The burden is on YOU to opt-out... that is how to say "no" if the company wants to sell or share your personal information to other businesses (third party non-affiliates). If you say nothing, or you throw the privacy notice in the filing cabinet or in the trash, it means "yes, you can share my personal information (such as your address, birth date, Social Security number, credit rating, spending habits, and so on) with any company you would like." So, the next time you get a privacy notice in the mail, make an affirmative decision on how you would like to share your personal information!

25. Magazines, credit card companies, clubs and organizations, charities, manufacturers and retailers make lists of their subscribers, customers, members and donors available to other businesses for a fee. Your information is reproduced and sold in countless ways. You should always exercise caution when you are making personal identifying information available by utilizing the Internet, mailing a

rebate/survey/warranty card, entering a drawing or sweepstakes, donating money, and even subscribing to magazines.

26. When in public places, always be aware of your surroundings. Thieves commonly use a distraction in cramped public places, such as elevators, escalators and revolving doors to "bump and lift" your money, identification, and credit cards. Be especially cautious with bags and purses that can be an easy target for a thief to "grab and run."

If you have any further questions or concerns,
or if you would like additional information, please contact:

Iowa Attorney General Tom Miller
Consumer Protection Division
Hoover State Office Building
1305 East Walnut Street
Des Moines, IA 50319
www.IowaAttorneyGeneral.org
Consumer@AG.State.IA.US
515-281-5926

This publication originates from the Privacy Rights Clearinghouse, 5384 Linda Vista Road, Suite 306, San Diego, CA 92110; phone: 619-298-3396; e-mail: www.privacyrights.org. With their consent, it has been adapted for Iowa consumers, edited and distributed by the Consumer Protection Division of the Office of Attorney General Tom Miller, Iowa Department of Justice. August 2007